Security Advisory

VxWorks security updates in Bosch Rexroth controllers

1 Advisory Information

Advisory ID: BOSCH-SA-761722

CVE Numbers and Scores:

- CVE-2019-12256
  - CVSS v3.0 Base Score: 9.8 (Critical)
- CVE-2019-12257
  - CVSS v3.0 Base Score: 8.8 (High)
- CVE-2019-12255
  - CVSS v3.0 Base Score: 9.8 (Critical)
- CVE-2019-12260
  - CVSS v3.0 Base Score: 9.8 (Critical)
- CVE-2019-12261
  - CVSS v3.0 Base Score: 8.8 (High)
- CVE-2019-12263
  - CVSS v3.0 Base Score: 8.1 (High)
- CVE-2019-12258
  - CVSS v3.0 Base Score: 7.5 (High)
- CVE-2019-12259
  - CVSS v3.0 Base Score: 6.3 (Medium)
- CVE-2019-12262
  - CVSS v3.0 Base Score: 7.1 (High)
- CVE-2019-12264
  - CVSS v3.0 Base Score: 7.1 (High)
- CVE-2019-12265
  - CVSS v3.0 Base Score: 5.4 (Medium)

Published: 08 Aug 2019

Last Updated: 08 Aug 2019

2 Summary

For the VxWorks operating systems used in embedded controls by Bosch Rexroth, information about several critical vulnerabilities in the network protocol stack has been published on July 29, 2019. [1]

3 Affected Products

- Rexroth embedded controls CML75 with an MLC/XLC firmware version < 14V22 Patch 4,
- Rexroth embedded controls XM21, XM22, XM42 with an MLC firm-ware version < 14V22 Patch 4,
- Rexroth industrial PC VPB40.4 with a firmware version < 14V22 Patch 4,
- Rexroth embedded controls CML75, CML85 with an MTX firmware version (all versions)

Rexroth embedded controls of the CML10, CML20, CML25, CML40, CMP60, CMP70, CML45 series as well as CML65 and HCT/HCQ (MTX micro) are not affected.

4 Solution

4.1 Firmware Update (Device)

- Rexroth embedded controls with an MLC/XLC firmware: From MLC/XLC firmware version 14V22 Patch 4, all vulnerabilities have been fixed. Thus, it is recommended, to update your version to these versions as soon as possible.
- Rexroth embedded controls with an MTX firmware: The implementation of a bug fix for MTX firmware versions based on version 14V22 is currently in progress and is expected to be available in Q4/2019. Upon request, a preliminary version based on firmware version 14V22 can be provided.

4.2 Mitigations and Workarounds

In use cases in which a device update is not possible or not yet available, compensatory measures are recommended which prevent or at least complicate taking advantage of the vulnerability. Always define such compensatory measures individually, in the context of the operational environment.

Some possible measures are described in the “Security Manual Electric Drives and Controls”, for example the network segmentation (please see [2]). In general, it is highly recommended to implement the measures described in the “Security Manual Drives and Controls”.

5 Vulnerability Details

5.1 CVE-2019-12256 (Stack overflow)

This vulnerability corresponds to a IPNET security vulnerability: Stack overflow in the parsing of IPv4 packets’ IP options

- CVSS 3.0 Base Score: 9.8

Impact: A specially crafted IPv4 packet, containing invalid encoded SSRR/LSRR options, may cause call-stack overflow. No specific services beyond IPv4 protocol support is required.

5.2 CVE-2019-12257 (Heap overflow)

IPNET security vulnerability: Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc

- CVSS 3.0 Base Score: 8.8

Impact: A specially crafted DHCP packet may cause overflow of heap-allocated memory on VxWorks system using DHCP. The attacker must share LAN with the device as DHCP packets is not forwarded by IP-routers.

5.3 CVE-2019-12255 (TCP Urgent Pointer = 0 leads to integer underflow)

IPNET security vulnerability: TCP Urgent Pointer = 0 leads to integer underflow

- CVSS 3.0 Base Score: 9.8

Impact: A specially crafted TCP-segment with the URG-flag set may cause overflow of the buffer passed to recv(), recvfrom() or recvmsg() socket routines.

5.4 CVE-2019-12260 (TCP Urgent Pointer state confusion caused by malformed TCP AO option)

IPNET security vulnerability: TCP Urgent Pointer state confusion caused by malformed TCP AO option

- CVSS 3.0 Base Score: 9.8

Impact: A series of specially crafted TCP-segments where the last step is a TCP-segment with the URG-flag set may cause overflow of the buffer passed to recv(), recvfrom() or recvmsg() socket routines.

5.5 CVE-2019-12261 (TCP Urgent Pointer state confusion during connect() to a remote host)

IPNET security vulnerability: TCP Urgent Pointer state confusion during connect() to a remote host

- CVSS 3.0 Base Score: 8.8

Impact: A specially crafted response to the connection attempt, where also the FIN- and URG-flags are set is sent as a response. This may put the victim into an inconsistent state, which make it possible to send yet another segment that trigger a buffer overflow.

5.6 CVE-2019-12263 (TCP Urgent Pointer state confusion due to race condition)

IPNET security vulnerability: TCP Urgent Pointer state confusion due to race condition

- CVSS 3.0 Base Score: 8.1

Impact: A series of segments with and without the URG-flag set must arrive with a very specific timing while an application on the victim is receiving from the session. The victim must be using a SMP-kernel and two or more CPU-cores alternatively an uni-processor kernel where the receiving task and the network task executes at different priorities.

5.7 CVE-2019-12258 (DoS of TCP connection via malformed TCP options)

IPNET security vulnerability: DoS of TCP connection via malformed TCP options

- CVSS 3.0 Base Score: 7.5

Impact: A specially crafted packet containing illegal TCP-options can result in the victim not just dropping the TCP-segment but also drop the TCP-session.

5.8 CVE-2019-12259 (DoS via NULL dereference in IGMP parsing)

IPNET security vulnerability: DoS via NULL dereference in IGMP parsing

- CVSS 3.0 Base Score: 6.3

Impact: This vulnerability require that the TCP/IP-stack is assigned a multicast address the API intended for assigning unicast addresses or something with the same logical flaw is a prerequisite.

5.9 CVE-2019-12262 (Handling of unsolicited Reverse ARP replies (Logical Flaw))

IPNET security vulnerability: Handling of unsolicited Reverse ARP replies (Logical Flaw)

- CVSS 3.0 Base Score: 7.1

Impact: The RARP reception handler verifies that the packet is well formed, but fails to verify that the node has an ongoing RARP-transaction matching the received packet.

5.10 CVE-2019-12264 (Logical flaw in IPv4 assignment by the ipdhcpc DHCP client)

IPNET security vulnerability: Logical flaw in IPv4 assignment by the ipdhcpc DHCP client

- CVSS 3.0 Base Score: 7.1

Impact: The VxWorks DHCP client fails to properly validate that the offered IP-address in a DHCP renewal or offer response contains a valid unicast address. An attacker may assign multicast or broadcast addresses to the victim.

5.11 CVE-2019-12265 (IGMP Information leak via IGMPv3 specific membership report)

IPNET security vulnerability: IGMP Information leak via IGMPv3 specific membership report

- CVSS 3.0 Base Score: 5.4

Impact: An attacker can create specially crafted and fragmented IGMPv3 query report, which may result in the victim transmitting undefined buffer content.

6 Additional Resources

[1] ICS Advisory: Wind River VxWorks
[2] Bosch Rexroth Security Manual Drives and Controls
[3] Security Advisory: WIND RIVER TCP/IP STACK (IPNET) VULNERABILITIES

7 Revision History

08 Aug 2019: Initial Publication